EBU

OPERATING EUROVISION AND EURORADIO

# R 142

# CYBERSECURITY BEST PRACTICES FOR CONNECTED TELEVISIONS AND SERVICES

RECOMMENDATION

Geneva
April 2016

[*] Page intentionally left blank. This document is paginated for two sided printing

# Security Best Practices for Connected Televisions and Services

| *EBU Committee* | *First Issued* | *Revised* | *Re-issued* |
|---|---|---|---|
| TC | 2016 | | |

**Keywords:** SMART TV, Connected TV, HbbTV, Service, Security, Root Certificate, Sandboxing.

## Recommendation

***The EBU, considering that,***

1. Media companies increasingly provide HbbTV services that can be accessed via consumer TV sets.

2. The cyberthreats of malware and ransomware are increasingly easier to perform.

3. Connected media devices and connected TVs, in particular, tend to have a very low security threshold inherited from the era of non-connected broadcast media.

4. The uncovered vulnerabilities on connected TVs can, if exploited, damage both the reputation of the TV vendors and the service providers.

***Recommends that broadcasters and connected TV service providers:***

1. Use secure protocols (e.g. https) wherever necessary for the integrity and confidentiality for their connected TV services.

2. Implement the use of TLS root certificates for HbbTV services, as described in [1].

***The EBU further recommends that on connected TVs:***

3. If the websites use https for delivery, the device should not accept certificates from non-trusted roots. For HbbTV applications a list of TLS root certificates that must be supported by HbbTV terminals can be found in [1]. The same applies to the execution of script code (e.g. JavaScript) within the web browser or the HbbTV browser.

4. Processes should be segregated (functionalities that can be executed from a remote controller button should run in a separate process from system processes such as the browser).

5. Internet facing processes should always run as unprivileged (non-root accounts).

6. Unused or unneeded services should be disabled or deactivated by default.

7. All areas of the operating systems should be patchable and should be patched regularly. For older devices that are no longer supported by the manufacturer, clear messages

should at least advertise that there will be no more patches for these obsolete TV sets. A minimum amount of 5 years support is required for all connected TVs.

8. Anti-malware technologies should be installed.

9. Regular audits of the operating system and vendor applications should be performed to identify vulnerabilities and flaws, especially before releasing a final version.

10. A firmware reset should reset the complete device, including all file systems.

11. The underlying operating system should be hardened following best practices. If feasible, mandatory access controls (MAC) technologies such as SELinux should be integrated.

12. The web browser (web browser and/or web browser application) should make use of state-of-the-art web browser protection mechanisms such as:

    a. Sandboxing (for websites and plug-ins).

    b. Secure cookie handling.

    c. Anti-exploit technologies such as ASLR, DEP, SEH.

    d. Anti-malware technologies such as harmful website prevention.

## References

[1] http://dtg.org.uk/work/DBook_Resources/dtgrootcert.html